(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10003257 A**

(43) Date of publication of application: **06 . 01 . 98**

(51) Int. Cl **G09C 1/00**
G06F 1/00
G06F 17/60
H04L 9/32

(21) Application number: **08156964**

(22) Date of filing: **18 . 06 . 96**

(71) Applicant: **TOSHIBA CORP**

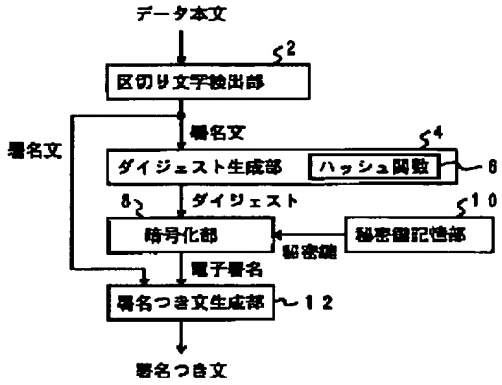
(72) Inventor: **KOGANEZAWA YUICHI**
KITAORI MASASHI

(54) **METHOD AND DEVICE FOR ADDING ELECTRONIC SIGNATURE, AND METHOD FOR VERIFYING ELECTRONIC SIGNATURE**

(57) Abstract:

PROBLEM TO BE SOLVED: To extract and quote the pair of a signed sentence/an electronic signature from an electronic document by adding the electronic signature against a data main sentence in a signature sentence unit.

SOLUTION: This electronic signature adding device is provided in the terminal device of the transmitter side and consists of a segmenting character detecting section 2, a digest generating section 4, a ciphering section 8, a secret key storage section 10 and a signed sentence generating section 12. When the signature information is added to the electronic sentence to prove that the sentence is written by the person who made the signature, the electronic sentence is divided into plural signed sentences using a beforehand decided specific character or a specific character column which appear in the sentence as a segment, signature information is generated based on the signed sentences for every divided signed sentence and the signature information is stored in accordance with the signed sentences. In other words, the electronic sentence, which is the signature object, is divided into plural signed sentences and an electronic signature is added to a signature sentence unit. Note that the specific character is at least one of a blank character, punctuation characters and parenthesis characters.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－3257

(43)公開日　平成10年(1998)１月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｂ	
			7259－5Ｊ			６４０Ｄ	
Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０Ｅ	
	17/60				15/21	Ｚ	
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ｂ	

審査請求　未請求　請求項の数10　ＯＬ　（全 17 頁）

(21)出願番号　特願平8－156964

(22)出願日　平成８年(1996)６月18日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　小金澤　雄一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　北折　昌司
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

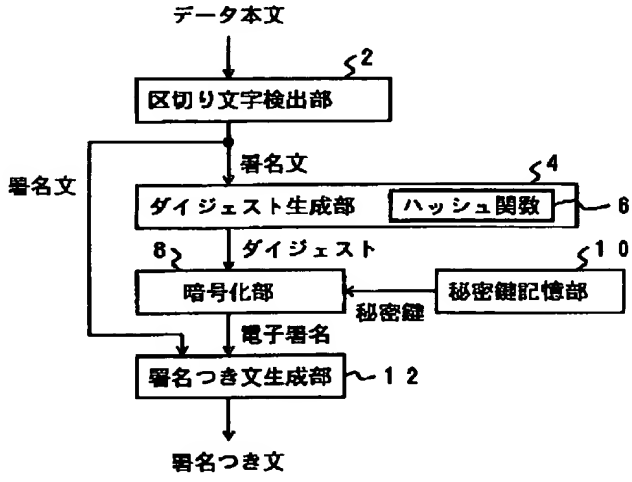
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　電子署名付加方法及び電子署名装置並びに電子署名検証方法

(57)【要約】

【課題】　電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする電子署名装置を提供すること。

【解決手段】　電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、電子化された文書を、該文書中に出現する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割し、分割された署名文ごとに、該署名文をもとに署名情報を生成し、前記署名文に対応付けて前記署名情報を格納することを特徴とする。



【特許請求の範囲】

【請求項１】電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、
電子化された文書を、該文書中に出現する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割し、
分割された署名文ごとに、該署名文をもとに署名情報を生成し、
前記署名文に対応付けて前記署名情報を格納することを特徴とする電子署名付加方法。

【請求項２】前記特定文字は、空白文字、句点文字、読点文字または括弧文字のうちの少なくとも１つであることを特徴とする請求項１に記載の電子署名付加方法。

【請求項３】電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、
署名情報を付加する対象となる文書中から予め定められた特定文字を除外し、
前記文書中から前記特定文字を除外して得られた文をもとに署名情報を生成し、
前記署名情報を付加する対象となる文書に、生成された前記署名情報を付加することを特徴とする電子署名付加方法。

【請求項４】前記特定文字は、空白文字、句点文字、読点文字、括弧文字および印刷不可能な制御文字のうちの少なくとも１つであることを特徴とする請求項３に記載の電子署名付加方法。

【請求項５】前記署名情報は、該署名情報のもととなる文から所定のハッシュ関数を用いて生成したダイジェストを公開鍵暗号方式の所定の秘密鍵で暗号化したものであることを特徴とする請求項１または３に記載の電子署名付加方法。

【請求項６】前記署名情報は、該署名情報による署名対象となる文の前方または後方に挿入することを特徴とする請求項１または３に記載の電子署名付加方法。

【請求項７】作者を証明する署名情報が付加された電子化された文書を受け取り、
受け取った前記文書中の印字可能文字の総数と印字不可能文字の総数をもとに所定の計算式を用いて前記署名情報の信頼性を評価することを特徴とする電子署名検証方法。

【請求項８】前記特定文字は、印刷不可能な文字であることを特徴とする請求項７に記載の電子署名検証方法。

【請求項９】前記所定の計算式は、ｐを印字不可能文字の種類、ｍを文書の文字数、ｋを印字不可能な文字の数、ｌをメッセージダイジェストのビット長、信頼性の値をＴとしたとき、Ｔ＝（ｐ＾ｋ）×（ｍ＋１）×（ｍ＋２）×…×（ｍ＋ｋ）／（２＾ｌ）で表されるものであり、求められた信頼性の値Ｔと予め定められたしきい値とを比較することにより前記署名情報の信頼性を評価することを特徴とする請求項７に記載の電子署名検証方法。

【請求項１０】電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名装置において、
電子化された文書を、該文書中に出現する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割する手段と、
分割された署名文ごとに、該署名文をもとに署名情報を生成する手段と、
前記署名文に対応付けて前記署名情報を格納する手段とを備えたことを特徴とする電子署名装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子化された文書データの送信・蓄積にあたって改ざんを防止するために作者を証明する署名データを該文書データに付加する電子署名付加方法及び電子署名装置、並びに電子署名の付加された電子化文書データの信頼性を評価する電子署名検証方法に関する。

【０００２】

【従来の技術】近年では、電子メールに代表されるように文書情報を電子化して（コード化して）送受信するような情報システムが広く普及している。受信された電子化文書情報は、通常、磁気記録媒体等に蓄積され、文書情報の一部を引用するなどの再利用をすることもできる。

【０００３】ところで、一般的に文書は、閲覧可能な者を限定する必要のある内容のものと、閲覧可能な者を不特定とする内容のものとに分けることができる。例えば、個々の企業や人の秘密に関するものを内容とする電子化文書情報が前者に該当するであろうし、企業や人あるいは公共機関などが第３者に知らせたい事柄に関するものを内容とする電子化文書情報が後者に該当するであろう。前者に該当する電子化文書情報は、例えば暗号化しておくことにより復号鍵を持たない者には内容を知られないようにすることができる。一方、後者に該当する電子化文書情報は、通常、平文のままで、誰でもアクセスできるようにされる。

【０００４】ここで、後者に該当する電子化文書情報は、その性質上から通常は平文であるため、不正に内容を改ざんされる危険性がある。特に、公的な情報（電子化された情報）はデマや意図的な情報操作の標的になり易く、万一、こうした不正が行われた場合の社会的影響は甚大であると考えられる。

【０００５】そこで、必要に応じて電子化文書には、その内容が改ざんされていないことなどを証明する電子署名データが付加される。この電子署名データにより、例えば「その電子化文書は確かに公共機関が作成したものであって不正に改ざんされた情報やデマではない」ことが証明される。

【０００６】以下では、電子メールを例にして電子署名

の原理を説明する。図１９に、従来の電子署名を適用した電子メールの処理の流れを示す。

（１）送信側では、データ本文を受信者に送る場合、データ本文を圧縮してダイジェスト（圧縮文）を生成し、このダイジェストを送信側の持つ秘密鍵で暗号化してデジタル署名と呼ばれるデータ（圧縮暗号文）を生成し、これをデータ本文に付加して送信する。

【０００７】（２）受信側では、データ本文に付加されたデジタル署名データを送信側の持つ秘密鍵に対応する公開鍵で復号して、もとのダイジェスト・データを生成するとともに、受信したデータ本文を圧縮してダイジェスト・データを生成する。そして、生成した２つのダイジェスト・データを比較することによって、データ本文が正しいかどうかを判定することができる。

【０００８】このように電子署名は、（１）情報が改変されておらず、原情報のまま正しいものであることを保証するメッセージ認証の機能と、（２）情報の生成・伝送・処理・記憶・判断などの行為に関与した実体Ａ（エンティティＡ、例えばＡという人）が、そのエンティティＡであることを保証する機能であるエンティティ認証との両方の機能を持つものである。

【０００９】すなわち、エンティティＡとＢの間で、作成者をＡとする情報について何らかの問題が発生した場合に、（１）問題となっているメッセージの送り主が確かにＡであることをＢ側で証明できる機能を持ち、またＢがその事実を明示する証拠を呈示することができ、かつ、（２）Ｂが「にせ」のメッセージを偽造して、「そのメッセージの送り主がＡである」と主張することができないことをいう。

【００１０】次に、図２０を参照しながら、送信側での＊署名データの生成手順についてより詳しく説明する。まず、署名対象となる本文全体１００１は、ハッシュ関数１００２と呼ばれる変換処理によって圧縮文１００３すなわちダイジェスト１００３となる。

【００１１】ここで、ハッシュ関数とは、任意長のデジタルデータを一定長のデジタルデータに変換する一方向性関数であり、変換後のデータからもとのデータを推定することが極めて困難な点と、変換後のデータが予測困難な乱数である点に特徴がある。これによって、長いデジタルデータの全てを暗号化により署名する必要はなく、ハッシュ関数が生成した一定長のデジタルデータすなわちメッセージダイジェストを暗号化しさえすれば、全体のデータに署名したのと等価な効果が期待できるものである。良く用いられているハッシュ関数としてはＭＤ５（参考文献：RFC1321 The MD5 Message-Digest Algorithm）があげられる。

【００１２】次に、ダイジェスト１００３は本人だけが知る情報を鍵１００４として暗号化される。ここで使われるのが非対称鍵暗号方式の秘密鍵であり、なかでもＲＳＡ方式が良く用いられる。

【００１３】上記のようにして生成された署名１００５は、本文とともに送信され（図中１０６）、受信側で検証されることになる。ここで、上記のＲＳＡ方式について簡単に説明する。

【００１４】ＲＳＡは、R.L.Rivest,A,Shamir,L.Adleman によって考案されたシステムで、この手法はモジュロ指数に依存している。公開指数と算術モジュロからなるパラメータ対を公開鍵、秘密指数と算術モジュロからなるパラメータ対を秘密鍵と呼び、以下の記号および略号

Ｘ，Ｙ　：データブロック。算術モジュロより小さい。
ｎ　：算術モジュロ
ｅ　：公開指数
ｄ　：秘密指数
ｐ，ｑ　：素数。この積が算術モジュロ（ｎ）となる。
ｌｃｍ　：最小公倍数
ｍｏｄ　ｎ　：算術モジュロｎ

を用いて、この非対称アルゴリズムは、次のような、データブロックの転送のための指数関数を使用する。

Ｙ＝Ｘ＾ｅ　ｍｏｄ　ｎ　（ただし、０≦Ｘ＜ｎ）
Ｘ＝Ｙ＾ｄ　ｍｏｄ　ｎ　（ただし、０≦Ｙ＜ｎ）

例えば、これは下記の解によって満足される。

ｅｄ　ｍｏｄ　ｌｃｍ（ｐ－１，ｑ－１）＝１　または
ｅｄ　ｍｏｄ　（ｐ－１）（ｑ－１）＝１

この処理を有効にするために、データブロックは整数と解釈されなくてはならない。

【００１５】ここで、公開されるのは（ｅ，ｎ）であり、秘密鍵はｄである。署名では秘密鍵ｄを使ってダイジェストが暗号化される。誰でもダイジェストを生成することはできるが、公開されている（ｅ，ｎ）から秘密鍵ｄを導くことは非常に困難であるため、署名は秘密鍵ｄを知る本人だけが事実上行うことができる。しかるに、（ｅ，ｎ）は公開されており、これらが上記所定の計算式を満たす関係にあることから、誰でも暗号を解くことが可能となり、署名を検証することができるのである。

【００１６】次に、図２１を参照しながら、受信側での署名検証の手順についてより詳しく説明する。受信側では、受け取った署名つき文１００６中の本文から所定のハッシュ関数１００２によりダイジェスト１（図中１０１１）を生成する。一方、本文に添付された署名をＲＳＡ公開鍵１０１０を用いて暗号を解くことによって、本文の著者である本人が生成した圧縮文であるダイジェス

ト２（図中１０１２）を作り出す。そして、両者の一致を見ることによって（１０１３）、一致していれば本文が署名を作った人物によって作られた文章であることが示され（１０１４）、また一致していなければ署名が間違っている、すなわち誰かが改ざんしたことを検出することが可能となる（１０１５）。

【００１７】このように電子署名は文章の改ざんを防止し、文章の内容の信頼性を保つことができる。しかしながら、上記のような従来の電子署名は文章全体に対して行われるため、文章全体からある文を部分的に引用した場合、電子署名はその部分に対して全く役にたたなくなってしまうという問題点があった。特に、引用された部分が意味のある重要なものである場合、改ざんの有無等を検出できないことは非常に不都合である。

【００１８】より具体的に説明すると、例えば図２２にしめされるように、Ａが作成した文１、文２、文３からなる文章全体に電子署名Ｘを付加してＢに転送したとする。その後、ＢがＡにより作成された文章中から文２のみを引用して、文ａ、文２、文ｂからなる文章を作成し、これに電子署名Ｙを付加してＣに転送したとする（ここで、文ａ中に、文２の作成者はＡであることが書かれていたものとする）。この場合、Ｃにとっては、Ｂの言う通り本当に文２の作成者がＡであるのか否かについて認証不能となる。

【００１９】また、上記のような不都合を回避するためには、例えば上記の具体例で言うと、Ｂは文２だけをＣに転送するために、文１、文２、文３からなる文章全体とその電子署名を転送する必要があり、非常に不都合である。

【００２０】一方、上記のような引用については他の問題点がある。すなわち、例えば文章全体を引用した際に、編集等の結果として空白や改行といった文書の意味に関与しない制御文字が意識しないところで挿入された場合、あるいは印刷により印字できない文字を含んでいる場合のように、意図しない改ざんが行われたような場合、文書の意味は全く変えられていないにもかかわらず、従来の電子署名メカニズムでは文書が改ざんされたものとして検出してしまう。しかし、このように文書の意味が変えられていない場合には、改ざんされていないものとして検出するような電子署名メカニズムが提供されれば、非常に有用性が高い。

【００２１】次に、従来の電子署名のさらに他の問題点について述べる。改ざんをもくろむ者は、改ざんした文書のメッセージダイジェストが改ざん前のメッセージダイジェストに一致するように改ざんを工夫する。そのために印字不可能な文字が使われる。すなわち、文書を改ざんするとともに、この文書中に印字不可能な文字をいくつか挿入することで、改ざんした文書の内容を変えずに同じメッセージダイジェストを作ることが不可能とは言えない。

【００２２】例えば、「費用は、１０，０００円です。」を「費用は１００，０００円です。」と改ざんしても、ダイジェストの不一致により改ざんが検出されるであろう。これに対して、「費用は、　１００，０００円です。」あるいは「　費用は、１００，０００円です。　」のように、いくつかの空白文字を挿入していけば、もとのダイジェストと一致するものを探し出せる可能性がある。

【００２３】しかしながら、従来は、電子署名の付加された文書の受信側において、上記のような改ざんの可能性あるいは文書の信頼性を示すような指標が全く与えられていなかった。

【００２４】

【発明が解決しようとする課題】上述したように従来では、電子署名は文章全体に対して行われるため、文章全体から一部引用した部分に対しては、認証不能であるという問題点があった。また、従来では、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うようなことができなかった。

【００２５】また、従来の電子署名では、文書を改ざんするとともに、この文書中に印字不可能な文字をいくつか挿入することで、もとの文書と同じメッセージダイジェストを作ることが不可能とは言えないが、この種の改ざんの可能性あるいは文書の信頼性を示すような指標が全く与えられていなかった。

【００２６】本発明は、上記事情を考慮してなされたもので、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする電子署名付加方法及び電子署名装置を提供することを目的とする。

【００２７】また、本発明は、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる電子署名付加方法及び電子署名装置を提供することを目的とする。

【００２８】また、本発明は、印刷にも有効な電子署名付加方法及び電子署名装置を提供することを目的とする。また、本発明は、本文中の印字不可能な文字の挿入による電子署名の信頼性低下を防ぐアルゴリズムを提供することによって、改ざんの可能性を見積もり、受信者に注意を促すことの可能な電子署名検証方法を提供することを目的とする。

【００２９】

【課題を解決するための手段】本発明（請求項１）は、電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、電子化された文書を、該文書中に出現する予め定められた特定文字また

は特定文字列を区切りとして、複数の署名文に分割し、分割された署名文ごとに、該署名文をもとに署名情報を生成し、前記署名文に対応付けて前記署名情報を格納することを特徴とする。

【００３０】本発明によれば、署名対象となる電子化文書を複数の署名文に分割し、署名文単位に電子署名を付加するので、電子化文書から署名文・電子署名対の単位で引用することが可能となる。

【００３１】本発明（請求項２）は、請求項１において、前記特定文字は、空白文字、句点文字、読点文字または括弧文字のうちの少なくとも１つであることを特徴とする。

【００３２】本発明（請求項３）は、電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、署名情報を付加する対象となる文書中から予め定められた特定文字を除外し、前記文書中から前記特定文字を除外して得られた文をもとに署名情報を生成し、前記署名情報を付加する対象となる文書に、生成された前記署名情報を付加することを特徴とする。

【００３３】本発明によれば、特定文字を適宜設定することにより、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる。

【００３４】また、本発明において、除外対象とする特定文字を印字不可能な文字すべてとすれば、印字可能文字をもって文書を改ざんすることが事実上不可能になる。また、印字された後も電子署名による改ざん防止に役立つ。

【００３５】本発明（請求項４）は、請求項３において、前記特定文字は、空白文字、句点文字、読点文字、括弧文字および印刷不可能な制御文字のうちの少なくとも１つであることを特徴とする。

【００３６】本発明（請求項５）は、上記各発明において、前記署名情報は、該署名情報のもととなる文から所定のハッシュ関数を用いて生成したダイジェストを公開鍵暗号方式の所定の秘密鍵で暗号化したものであることを特徴とする。

【００３７】本発明（請求項６）は、上記各発明において、前記署名情報は、該署名情報による署名対象となる文の前方または後方に挿入することを特徴とする。本発明（請求項７）に係る電子署名検証方法は、作者を証明する署名情報が付加された電子化された文書を受け取り、受け取った前記文書中の印字可能文字の総数と印字不可能文字の総数をもとに所定の計算式を用いて前記署名情報の信頼性を評価することを特徴とする。

【００３８】本発明によれば、印字可能文字の総数と印字不可能文字の総数をもとに電子署名の信頼性を計算し、改ざんの可能性を評価することができる。そして、必要に応じて警告を発するなどして注意を促すことができる。

【００３９】本発明（請求項８）は、請求項７において、前記特定文字は、印刷不可能な文字であることを特徴とする。本発明（請求項９）は、請求項７において、前記所定の計算式は、ｐを印字不可能文字の種類、ｍを文書の文字数、ｋを印字不可能な文字の数、ｌをメッセージダイジェストのビット長、信頼性の値をＴとしたとき、Ｔ＝（ｐ＾ｋ）×（ｍ＋１）×（ｍ＋２）×…×（ｍ＋ｋ）／（２＾ｌ）で表されるものであり、求められた信頼性の値Ｔと予め定められたしきい値とを比較することにより前記署名情報の信頼性を評価することを特徴とする。

【００４０】本発明（請求項１０）は、電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名装置において、電子化された文書を、該文書中に出現する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割する手段と、分割された署名文ごとに、該署名文をもとに署名情報を生成する手段と、前記署名文に対応付けて前記署名情報を格納する（前方または後方に挿入する）手段とを備えたことを特徴とする。

【００４１】上記の方法に係る各発明は、装置に係る発明としても成立する。なお、以上の各発明について、相当する処理手順を実行させるプログラムを、コンピュータを制御するためのプログラムとしてコンピュータ読取可能な記憶媒体に格納し、コンピュータに該記憶媒体からプログラムを読取らせ、コンピュータ上で実行させることが可能である。

【００４２】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。以下で説明する各実施形態の送受信システムは、電子化文書を送信する送信側となる端末装置と、この電子化文書を受信する受信側となる端末装置と、これらをつなぐ媒体から構成される。もちろん、端末装置に送信機能及び受信機能の両方を設けても良い。媒体は、ネットワークであっても良いし、フロッピー・ディスクあるいはＣＤ－ＲＯＭなど可搬性の情報記録媒体であっても良いし、少なくとも一部または全部に無線通信部分を含んでいても良い。また、送信側となる端末装置から一旦、所定のサーバ装置等に蓄積され、その後、サーバ装置等から受信側となる端末装置に転送される形態でも良い。端末装置は、媒体に応じた送信装置、受信装置を持つものとする。

【００４３】本実施形態において、署名文とは、署名対象となる一纏まりの文のことを言うものとする。また、処理後署名文とは、署名文から予め定められた文字を除外した文のことを言うものとする。第１の実施形態では、署名文からダイジェストを生成するのに対して、第

２の実施形態では、処理後署名文からダイジェストを生成する。なお、署名文も処理後署名文も平文である。

【００４４】本実施形態において、データ本文とは、署名対象となる一纏まりの文書全文（平文）を言うものとする。また、署名つき文とは、電子署名の付加された署名文を連結したものを言うものとする。言い換えると、署名対象となるデータ本文に、署名文単位に生成された電子署名が付加あるいは挿入された文を言うものとする。

【００４５】（第１の実施形態）第１の実施形態では、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする発明の実施形態について説明する。

【００４６】まず、本実施形態の電子署名付加装置（電子署名装置）について説明する。図１は、本電子署名付加装置の構成を示す図である。また、図２は、本電子署名付加装置による署名付加処理の手順を示すフローチャートである。

【００４７】電子署名付加装置は、送信側の端末装置内に設けられる。図１に示すように、電子署名付加装置は、区切り文字検出部２、ダイジェスト生成部４、暗号化部８、秘密鍵記憶部１０、署名つき文生成部１２を備えている。

【００４８】図１中のデータ本文は、署名を付加する本文全体であり、複数の文章や段落などから構成されている通常の文書である。区切り文字検出部２は、データ本文から予め定められた位置または複数の区切り文字を検出し、データ本文を、該区切り文字を末尾とする適当な長さの署名文に区切って行く（ステップＳ１１）。

【００４９】検出する区切り文字としては、任意の位置または複数のものを定義することができる。例えば、検出する区切り文字として、ピリオド“　．”および読点“。”を用いる。もちろん、ピリオド“　．”および読点“　。”の一方だけ定めても有効な場合もある。あるいは、文末文字“　ＡＳＣＩＩ：ｎｌ＝０Ａ（ｈｅｘ）　”および段落末文字“　ＡＳＣＩＩ：ｃｒ＝０Ｄ（ｈｅｘ）　”の一方だけを用いる方法もある。また、上記ピリオド“　．”および読点“　。”の少なくとも一方に、さらに句点“　、”、閉じる括弧“　］　”、“　｝　”、“）　”や文末文字“　ＡＳＣＩＩ：ｎｌ＝０Ａ（ｈｅｘ）　”や段落末文字“ＡＳＣＩＩ：ｃｒ＝０Ｄ（ｈｅｘ）　”の少なくとも一つを加えて、適宜定義することができる。もちろん、この他にも種々の区切り文字の定義が可能である。

【００５０】図３に、本区切り文字検出部２の処理手順の一例を示す。予め区切り文字を定め（例えば句点“　、”と読点“　。”とする）、これを区切り文字リスト１４に登録しておく。まず、データ本文中から一文字入力しバッファ（図示せず）に入れる（ステップＳ２１）。ここで、バッファに入力した文字が区切り文字リスト１４に登録された文字であるか否かを判定し（ステップＳ２２）、区切り文字でなかった場合、データ本文中から次の一文字を入力しバッファに入れる。

【００５１】上記の処理を繰り返し、ステップＳ２２でバッファに入れた文字が区切り文字であった場合（例えば句点“　、”または読点“　。”であった場合）に、バッファを出て（ステップＳ２３）、１つの署名文（例えば句点“　、”または読点“　。”を末尾とするもの）が得られる。

【００５２】ダイジェスト生成部４は、既に説明したようなハッシュ関数６によって署名文から、ダイジェストを生成する（ステップＳ１２）。用いるハッシュ関数、ダイジェストのビット長は、予め決めておくものとする。本実施形態では、ハッシュ関数６として「ＭＤ５」を用い、ダイジェストのビット長は１２８ビットとする。ハッシュ関数としてＳＨＡを用いる場合は、ダイジェストのビット長は１６０ビットとなる。また、ハッシュアルゴリズムとして他のものを用いても構わない。なお、用いるハッシュ関数を選択可能として、実際に用いたハッシュ関数（あるいはハッシュ関数とダイジェストのビット長）を示す情報を署名つき文に付加することも可能である。

【００５３】暗号化部８は、秘密鍵記憶部１０に記憶されている公開鍵暗号方式の秘密鍵を用いてダイジェストを暗号化する（ステップＳ１３）。この暗号化されたダイジェストが電子署名として用いられる。ここでは、公開鍵暗号方式としてＲＳＡ方式を用いることとする。

【００５４】ここで、セキュリティー上、上記秘密鍵は他人に知得されないようにするのが好ましい。例えば、上記秘密鍵記憶部１０としてＩＣカードを用い、ＩＣカードに上記秘密鍵を記録しておき、必要時に、例えば本署名付加処理を行うときに、該ＩＣカードをＩＣカード・リーダー（図示しない）にセットし、ＩＣカード・リーダーから読み取った秘密鍵を暗号部８に渡すようにする。

【００５５】署名つき文生成部１２は、区切り文字検出部２にて得られた署名文夫々に対して電子署名を付加して行く（ステップＳ１４）。ここでは、署名文の後に電子署名を挿入して署名つき文を生成するものとする。なお、署名文の前に電子署名を挿入しても良いし、電子署名をまとめて全文書の前にヘッダとして挿入しても良い。

【００５６】そして、ステップＳ１５で、現在の署名文がデータ本文の最後の文章かどうかを判定する。最後でなければ再び区切りステップＳ１１の文字列検出部２による処理に戻り、ステップＳ１５でデータ本文が終りとなるまでステップＳ１１～ステップＳ１４の処理を繰り返す。

【００５７】この結果、例えば図４に示すような署名つき文を得ることができる。ここでは、署名文（分割メッ

セージ）の後に電子署名を挿入した結果、データ本文中の適当な間隔に署名が挿入された形になっている。

【００５８】なお、電子署名中には、それが電子署名のデータであることが判るような情報を含ませることが望ましい。例えば、電子署名本体（ダイジェストを暗号化したデータ）を“＃＃Ｓｉｇｎａｔｕｒｅ＝”と“＃＃”で挟んだデータを用いることができる。

【００５９】また、各署名文には、先頭のものからの序列を示すシーケンス番号（およびシーケンス番号であることを示す所定の情報；例えば＃＃ＳＮ＝”と“＃＃”でシーケンス番号を挟む）を付加しても良い（例えば各署名文の直前）。このようにすると、受信側での処理（例えば署名文の分割処理）が容易となる。また、上記のように電子署名をまとめて全文書の前にヘッダとして挿入する場合、ヘッダ内でシーケンス番号を用いて署名文と電子署名との対応を取ることができる。

【００６０】次に、本実施形態の電子署名検証装置について説明する。図５は、本実施形態の電子署名検証装置の構成を示す図である。また、図６は、本電子署名検証装置による署名検証処理の手順を示すフローチャートである。

【００６１】電子署名検証装置は、受信側の端末装置内に設けられる。図５に示すように、電子署名検証装置は、署名分割部２２、ダイジェスト生成部２４、復号部２８、公開鍵記憶部３０、比較部３２を備えている。

【００６２】図５中の署名つき文は、所定の媒体を通じて受け取った電子化文書であり、前述の電子署名付加装置によって電子署名が付加された文書である。電子署名は例えば図４のように文書中の適当な位置に挿入されている。

【００６３】署名分割部２２は、署名つき文から、１組の署名文と電子署名を取り出す（ステップＳ３１）。これには幾つかの方法が考えられる。１つは、電子署名が付加されたときに区切り文字検出部２により用いられたものと同一の処理を用いて署名文を取り出すとともに、署名文の前あるいは後などの決められた位置に付加されている所定ビット長の電子署名を取り出す方法である。他の１つは、例えば前述のように電子署名の一部に“＃＃Ｓｉｇｎａｔｕｒｅ＝”と“＃＃”からなるラベルを付加した場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。さらに他の方法は、各署名文に＃＃ＳＮ＝”と“＃＃”からなるラベルで挟まれたシーケンス番号が付加されている場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。

【００６４】次に、復号部２８は、公開鍵記憶部３０に記憶されている公開鍵暗号方式の公開鍵を用いて電子署名を復号するして、ダイジェスト（ダイジェスト＃１とする）に戻す（ステップＳ３２）。

【００６５】ここで、公開鍵は、電子署名が付加されたときに暗号化部８により用いられた秘密鍵に対応するものを用いる。例えば、暗号化の際に公開鍵暗号方式（ＲＳＡ）の秘密鍵が用いられた場合、該秘密鍵に一意に対応する公開鍵暗号方式（ＲＳＡ）の公開鍵を用いる。この公開鍵は、例えば署名つき文に付加された情報（例えば本文書の作成者の持つユーザＩＤあるいは送信元アドレスなど）をたよりに公開鍵サーバあるいは公開鍵データベースなどから入手できるものとする。

【００６６】一方、ダイジェスト生成部２４は、電子署名が付加されたときにダイジェスト生成部４により用いられたものと同一のハッシュ関数によって、取り出した署名文に対するダイジェスト（ダイジェスト＃２とする）を生成する（ステップＳ３３）。

【００６７】ここで、復号部２８によるダイジェスト＃１の生成処理と、ダイジェスト生成部２４によるダイジェスト＃２の生成処理とは、いずれを先に行っても良いし、並列実行しても良い。

【００６８】比較部３２は、ダイジェスト＃１とダイジェスト＃２の比較を行う（ステップＳ３４）。もし両者が一致すれば、その署名文は改ざんされていないので、その署名文に対する認証結果情報を、有効を示す情報（例えば１）とする（ステップＳ３５）。もし両者が不一致ならば、その署名文の改ざんを検出したことになるので、その署名文に対する認証結果情報を、無効を示す情報（例えば０）とする（ステップＳ３５）。認証結果情報は、例えば、該当する電子署名の直後にまたは直前に付加する方法、あるいは各署名文に＃＃ＳＮ＝”と“＃＃”からなるラベルで挟まれたシーケンス番号が付加されている場合、シーケンス番号と認証結果情報との対を記録して行く方法などが考えられる。

【００６９】以上の処理を、ステップＳ３７で文書の終りが検出されるまで、繰り返し行う。図７は、本電子署名検証装置による他の署名検証処理の手順を示すフローチャートである。本手順は、１つでも改ざんの検出された署名文が存在する場合、文書全体を無効とするようにした例である。

【００７０】この場合、ステップＳ３１～ステップＳ３４の比較と、ステップＳ３７での文書の終りの検出は、図６と同様であるが、図７の手順ではステップＳ３４の比較において一致がみられた場合、何も記録せず、ステップＳ３４の比較において不一致がみられた場合、その時点で異常終了とし、ステップＳ３７での文書の終りが検出され、全署名文について改ざんが検出されなかった場合に、正常終了とする。

【００７１】なお、各端末に、電子署名付加装置と電子署名検証装置の機能を持たせることが可能である。この場合、ダイジェスト生成部やハッシュ関数など構成部分の共通化を行うことができる。

【００７２】以上のように本実施形態によれば、データ本文に対し署名文単位に電子署名を付加するので、電子

化文書から署名文・電子署名の対の単位で抜き出して引用することが可能となる。

【００７３】（第２の実施形態）第２の実施形態では、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とするのに加え、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができるようにした発明の実施形態について説明する。

【００７４】まず、本実施形態の電子署名付加装置について説明する。図８は、本電子署名付加装置（電子署名装置）の構成を示す図である。また、図９は、本電子署名付加装置による署名付加処理の手順を示すフローチャートである。

【００７５】電子署名付加装置は、送信側の端末装置内に設けられる。図８に示すように、電子署名付加装置は、区切り文字検出部１０２、ダイジェスト生成部１０４、暗号化部１０８、秘密鍵記憶部１１０、署名つき文生成部１１２を備えている。

【００７６】図８中のデータ本文は、署名を付加する本文全体であり、複数の文章や段落などから構成されている通常の文書である。区切り文字検出部１０２は、データ本文から予め定められた位置または複数の区切り文字を検出し、データ本文を、該区切り文字を末尾とする適当な長さの署名文に区切って行くとともに、印字不可能文字除外部１０３を用いて予め定められた印字不可能文字を署名文から除外した処理後署名文を生成する（ステップＳ１１１）。

【００７７】検出する区切り文字としては、任意の位置または複数のものを定義することができる。例えば、検出する区切り文字として、ピリオド“　．”および読点“。”を用いる。もちろん、ピリオド“　．”および読点“　。”の一方だけ定めても有効な場合もある。あるいは、文末文字“　ＡＳＣＩＩ：ｎｌ＝０Ａ（ｈｅｘ）　”および段落末文字“　ＡＳＣＩＩ：ｃｒ＝０Ｄ（ｈｅｘ）　”の一方だけを用いる方法もある。また、上記ピリオド“　．”および読点“　。”の少なくとも一方に、さらに句点“　、”、閉じる括弧“　］　”、“　｝　”、“）　”や文末文字“　ＡＳＣＩＩ：ｎｌ＝０Ａ（ｈｅｘ）　”や段落末文字“ＡＳＣＩＩ：ｃｒ＝０Ｄ（ｈｅｘ）　”の少なくとも一つを加えて、適宜定義することができる。もちろん、この他にも種々の区切り文字の定義が可能である。

【００７８】区切り文字検出部１０２により署名文を生成する処理手順の一例は図３と同様である。すなわち、予め区切り文字を定め、これを区切り文字リスト１１４に登録しておく。まず、データ本文中から一文字入力しバッファ（図示せず）に入れる（ステップＳ２１）。ここで、バッファに入力した文字が区切り文字リスト１１４に登録された文字であるか否かを判定し（ステップＳ２２）、区切り文字でなかった場合、データ本文中から次の一文字を入力しバッファに入れる。

【００７９】次に、区切り文字検出部１０２により文書の区切り検出と署名に加味しない文字の排除を行って処理後署名文を生成する処理手順の一例について説明する。図１０は、区切り文字検出部１０２により処理後署名文を生成する処理手順の一例を示す。

【００８０】署名対象となるデータ本文から、まず、一文字の入力文字を取り出し（ステップＳ１２１）、印字不可能リスト１１３を参照して、その文字が予め定められた印字不可能文字か否かを検出する（ステップＳ１２２）。

【００８１】ここで、印字可能な文字は、少なくとも何らかの印字が行われる文字であり、ａ，ｂ，ｃ，…，１，２，３，…，あ，い，う，…，吾，亜，阿，…，などである。一方、印字不可能な文字は、空白、タブ、改行など、何の印字もされない文字である。例えば、後者の文字をＡＳＣＩＩコード表で表すと図１１中で太線で囲った範囲のものとなる。

【００８２】印字不可能な文字をすべて印字不可能リスト１１３に登録しておく。この印字不可能リスト１１３を参照することによって署名に加味しない文字が除外される。なお、除外対象とする印字不可能な文字を予め定めた一部のものとし、それらを印字不可能リスト１１３に登録しておくことも可能である。例えば、改行文字は除外しないようにすることができる。

【００８３】次に、文字リスト１１４を参照して、文字の区切りであるか否かが検出される（ステップＳ１２３）。なお、区切り文字として採用した文字は、このアルゴリズムを用いる場合には、印字不可能リスト１１３から除外する。もしステップＳ１２３の区切り検出をステップＳ１１２の印字可能検出より前に行う場合は、印字不可能リスト１１３の中に区切り文字が含まれていても構わない。

【００８４】さて、ステップＳ１２３で区切り文字でなかった場合、その文字はバッファ（図示せず）に蓄えられ（ステップＳ１２４）、ステップＳ１２１に戻って、次の一文字が取り出され、同様の処理が繰り返される。

【００８５】一方、ステップＳ１２３で区切り文字であった場合は、処理後署名文が形成されたことになるので、バッファをフラッシュして、以後の処理に署名文書を引き渡す（ステップＳ１２５）。このようにして、本文中から処理後署名文を取り出すことができる。

【００８６】なお、区切り文字検出部１０２による署名文の生成と処理後署名文の生成は、どのような順序で行っても良いし、同時に行っても良い。また、まず、署名文を生成し、生成された署名文から予め定められた印字不可能文字を除外することによって処理後署名文を生成しても良い。また、例えば、図３のフローチャートと図

１０のフローチャートをもとに、署名文と処理後署名文を同時に生成するフローチャートを作り出すことも容易である（この場合、署名文用と処理後署名文用の２つのバッファを用いる）。

【００８７】なお、上記では、区切り文字検出部１０２は、区切り文字を検出しているが、その代わりに、区切り文字列を検出するようにしても良い。例えば、読点“　。”や改行文字が単独で現れただけでは文の区切りとせず、読点“　。”と改行文字が続けて現れた場合に文の区切りとする。

【００８８】次に、ダイジェスト生成部１０４は、既に説明したようなハッシュ関数１０６によって処理後署名文からダイジェストを生成する（ステップＳ１１２）。用いるハッシュ関数、ダイジェストのビット長は、予め決めておくものとする。本実施形態では、ハッシュ関数１０６として「ＭＤ５」を用い、ダイジェストのビット長は１２８ビットとする。ハッシュ関数としてＳＨＡを用いる場合は、ダイジェストのビット長は１６０ビットとなる。また、ハッシュアルゴリズムとして他のものを用いても構わない。なお、用いるハッシュ関数を選択可能として、実際に用いたハッシュ関数（あるいはハッシュ関数とダイジェストのビット長）を示す情報を署名つき文に付加することも可能である。

【００８９】暗号化部１０８は、秘密鍵記憶部１１０に記憶されている公開鍵暗号方式の秘密鍵を用いてダイジェストを暗号化する（ステップＳ１１３）。この暗号化されたダイジェストが電子署名として用いられる。ここでは、公開鍵暗号方式としてＲＳＡ方式を用いることとする。

【００９０】ここで、セキュリティー上、上記秘密鍵は他人に知得されないようにするのが好ましい。例えば、上記秘密鍵記憶部１１０としてＩＣカードを用い、ＩＣカードに上記秘密鍵を記録しておき、必要時に、例えば本署名付加処理を行うときに、該ＩＣカードをＩＣカード・リーダー（図示しない）にセットし、ＩＣカード・リーダーから読み取った秘密鍵を暗号部１０８に渡すようにすることができる。

【００９１】署名つき文生成部１１２は、区切り文字検出部１０２にて得られた署名文夫々に対して電子署名を付加して行く（ステップＳ１１４）。ここでは、署名文の後に電子署名を挿入して署名つき文を生成するものとする。なお、署名文の前に電子署名を挿入しても良いし、電子署名をまとめて全文書の前にヘッダとして挿入しても良い。

【００９２】そして、ステップＳ１１５で、現在の署名文がデータ本文の最後の文章かどうかを判定する。最後でなければ再び区切りステップＳ１１１の文字列検出装置１０２による処理に戻り、ステップＳ１１５でデータ本文が終りとなるまでステップＳ１１１～ステップＳ１１４の処理を繰り返す。

【００９３】この結果、例えば図３に示すような署名つき文を得ることができる。ここでは、署名文の後に電子署名を挿入する結果、データ本文中の適当な間隔に署名が挿入された形になっている。

【００９４】なお、電子署名には、それが署名文のデータではなく電子署名のデータであることが判るような情報を含ませることが望ましい。例えば、電子署名本体を“＃＃Ｓｉｇｎａｔｕｒｅ＝”と“＃＃”で挟んだデータを用いることができる。

【００９５】また、各署名文には、先頭のものからの序列を示すシーケンス番号（およびシーケンス番号であることを示す所定の情報；例えば＃＃ＳＮ＝”と“＃＃”でシーケンス番号を挟む）を付加しても良い（例えば各署名文の直前）。このようにすると、受信側での処理（例えば署名文の分割処理）が容易となる。また、上記のように電子署名をまとめて全文書の前にヘッダとして挿入する場合、ヘッダ内でシーケンス番号を用いて署名文と電子署名との対応を取ることができる。

【００９６】次に、本実施形態の電子署名検証装置について説明する。図１２は、本実施形態の電子署名検証装置の構成を示す図である。また、図１３は、本電子署名検証装置による署名検証処理の手順を示すフローチャートである。

【００９７】電子署名検証装置は、受信側の端末装置内に設けられる。図１３に示すように、電子署名検証装置は、署名分割部１２２、印字不可能文字除外部１２３、ダイジェスト生成部１２４、復号部１２８、公開鍵記憶部１３０、比較部１３２を備えている。

【００９８】図１２中の署名つき文は、所定の媒体を通じて受け取った電子化文書であり、前述の電子署名付加装置によって電子署名が付加された文書である。電子署名は例えば図４のように文書中の適当な位置に挿入されている。

【００９９】署名分割部１２２は、署名つき文から、１組の署名文と電子署名を取り出す（ステップＳ１３１）。これには幾つかの方法が考えられる。１つは、電子署名が付加されたときに区切り文字検出部２により用いられたものと同一の処理を用いて署名文を取り出すとともに、署名文の前あるいは後などの決められた位置に付加されている所定ビット長の電子署名を取り出す方法である。他の１つは、例えば前述のように電子署名の一部に“＃＃Ｓｉｇｎａｔｕｒｅ＝”と“＃＃”からなるラベルを付加した場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。さらに他の方法は、各署名文に＃＃ＳＮ＝”と“＃＃”からなるラベルで挟まれたシーケンス番号が付加されている場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。

【０１００】次に、復号部１２８は、公開鍵記憶部１３

０に記憶されている公開鍵暗号方式の公開鍵を用いて電子署名を復号するして、ダイジェスト（ダイジェスト＃１とする）に戻す（ステップＳ１３２）。その際、公開鍵は、電子署名が付加されたときに暗号化部１０８により用いられた秘密鍵に対応するものを用いる。例えば、暗号化の際に公開鍵暗号方式（ＲＳＡ）の秘密鍵が用いられた場合、該秘密鍵に一意に対応する公開鍵暗号方式（ＲＳＡ）の公開鍵を用いる。この公開鍵は、前述したように、例えば署名つき文に付加された情報をたよりに入手できるものとする。

【０１０１】一方、印字不可能文字除去部１２３は、電子署名が付加されたときに印字不可能文字除外部１０３により用いられたものと同一の印字不可能リスト１１３を用いて、署名文から予め定められた印字不可能文字を除外して、処理後署名文を生成する（ステップＳ１３３－１）。

【０１０２】そして、ダイジェスト生成部１２４は、電子署名が付加されたときにダイジェスト生成部１０４により用いられたものと同一のハッシュ関数によって、生成された処理後署名文に対するダイジェスト（ダイジェスト＃２とする）を生成する（ステップＳ１３３－２）。

【０１０３】ここで、復号部１２８によるダイジェスト＃１の生成処理と、印字不可能文字除去部１２３およびダイジェスト生成部１２４によるダイジェスト＃２の生成処理とは、いずれを先に行っても良いし、並列実行しても良い。

【０１０４】比較部１３２は、ダイジェスト＃１とダイジェスト＃２の比較を行う（ステップＳ１３４）。もし両者が一致すれば、その署名文は改ざんされていないので、その署名文に対する認証結果情報を、有効を示す情報（例えば1）とする（ステップＳ１３５）。もし両者が不一致ならば、その署名文の改ざんを検出したことになるので、その署名文に対する認証結果情報を、無効を示す情報（例えば0）とする（ステップＳ１３５）。認証結果情報は、例えば、該当する電子署名の直後にまたは直前に付加する方法、あるいは各署名文に＃＃ＳＮ＝”と“＃＃”からなるラベルで挟まれたシーケンス番号が付加されている場合、シーケンス番号と認証結果情報との対を記録して行く方法などが考えられる。

【０１０５】以上の処理を、ステップＳ１３７で文書の終りが検出されるまで、繰り返し行う。図１４は、本電子署名検証装置による他の署名検証処理の手順を示すフローチャートである。本手順は、１つでも改ざんの検出された署名文が存在する場合、文書全体を無効とするようにした例である。

【０１０６】ステップＳ１３１～ステップＳ１３４の比較と、ステップＳ１３７での文書の終りの検出は、図１３と同様であるが、図１４の手順ではステップＳ１３４の比較において一致がみられた場合、何も記録せず、ステップＳ１３４の比較において不一致がみられた場合、その時点で異常終了とし、ステップＳ１３７での文書の終りが検出され、全署名文について改ざんが検出されなかった場合に、正常終了とする。

【０１０７】なお、各端末に、電子署名付加装置と電子署名検証装置の機能を持たせることが可能である。この場合、ダイジェスト生成部やハッシュ関数など構成部分の共通化を行うことができる。

【０１０８】以上のように本実施形態によれば、データ本文に対し署名文単位に電子署名を付加するので、電子化文書から署名文・電子署名の対の単位で抜き出して引用することが可能となる。また、印字された後も電子署名による改ざん防止に役立つ。

【０１０９】また、本発明は、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる。

【０１１０】また、本実施形態において、印字不可能な文字をすべて除外対象とすれば、改ざんした文書に印字不可能文字を挿入してもとと同じダイジェストを作成することが不可能になる。

【０１１１】さて、第１の実施形態では、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする発明の実施形態について説明し、第２の実施形態では、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とするのに加え、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができるようにした発明の実施形態について説明したが、他の実施形態として、データ本文を署名文単位に分割せず、電子署名をデータ本文全体に対して付加するものであって、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができるようにした実施形態も可能である。

【０１１２】この場合の実施形態は、例えば、第２に実施形態において、区切り文字を検出して署名文を生成する構成部分、すなわちデータ本文を署名文単位に分割する構成部分を削除することで容易に構成可能である。すなわち、電子署名付加装置側では、データ本文から予め定められた印字不可能文字を削除して、ダイジェストを生成し、これを暗号化し、これによって得られた電子署名を該データ本文に付加すれば良い。一方、電子署名検証装置側では、受け取ったデータ本文から予め定められた印字不可能文字を削除して、ダイジェスト＃１を生成するとともに、データ本文に付加された電子署名を復号

してダイジェスト＃２を生成し、ダイジェスト＃１とダイジェスト＃２を比較すれば良い。

【０１１３】（第３の実施形態）第３の実施形態では、改ざんした文書に空白などの印字不可能文字を挿入してもとと同じダイジェストが作成された可能性についての指標を与えるようにした発明の実施形態について説明する。

【０１１４】従来例で説明したように、改ざんをもくろむ者は、改ざんした文書のメッセージダイジェストが改ざん前のメッセージダイジェストに一致するように改ざんを工夫する。そのために印字不可能な文字が使われる。

【０１１５】まず、文書の文字数をｍとする。この中に印字不可能な文字を一つ挿入することで、文書の内容自体を変えずに同じメッセージダイジェストを作ることができる可能性がある。不正に作られるダイジェストの数は、挿入する印字不可能な文字の種類ｐとこれを挿入する位置（ｍ＋１）の積により次式のように表される。

Ｌ＝ｐ×（ｍ＋１）

L_1 ＝（一つの印字不可能文字の付加によって作られるダイジェストの数）

ｐ＝（印字不可能文字の種類）

ｍ＝（文書の文字数）

２個の印字不可能文字を付加する場合、２個の組み合わせはｐの２乗通りあり、またその位置は１個目に可能な挿入位置（ｍ＋１）と２個目に可能な挿入位置の数（ｍ＋２）との積で近似できる。したがって、ｋ個の印字不可能文字が付加されている場合、不正に作ることができるダイジェストの数Ｌは、次式のように表される。

L_k ＝（ｐ＾ｋ）×（ｍ＋１）×（ｍ＋２）×…×（ｍ＋ｋ）

L_k ＝（ｋ個の印字不可能文字の付加によって作られるダイジェストの数）

ｐ＝（印字不可能文字の種類）

ｍ＝（文書の文字数）

ｋ＝（印字不可能な文字の数）

一方、メッセージダイジェストのビット長をｌとすると、正当な手段で作り出されるメッセージダイジェストの数は２＾ｌである。したがって、これに対する不正に作られるメッセージダイジェストの数L_kの割合が、メッセージダイジェストの信頼性の指数となる。

Ｔ＝（ｐ＾ｋ）×（ｍ＋１）×（ｍ＋２）×…×（ｍ＋ｋ）／（２＾ｌ）

ｐ＝（印字不可能文字の種類）

ｍ＝（文書の文字数）

ｋ＝（印字不可能な文字の数）

ｌ＝（メッセージダイジェストのビット長）

図１５は、Ｔ＝０．０００１、すなわち１万分の１以下の確率で改ざんが可能になると考えられる印字不可能な文字の最大数を、文書の文字数（有効文字数）とダイジェストのビット長をパラメータに計算した結果である。ここで、印字不可能な文字の種類は３４とした。

【０１１６】これによれば、１０００（ｎｅａｒｌｙ　ｅｑｕａｌ　２＾１０）文字の文書に対して１２８ビットのメッセージダイジェストを作った場合、印字不可能な文字が７文字以下ならばダイジェストの信頼度は十分（改ざん可能な確率は１万分の１以下）であることが判る。もちろん文書の種類によってはそれ以上の信頼度を必要とする場合がある。しかし、同様の計算を行うことで所望の信頼度を確保することが可能となる。この計算に用いたＣ言語によるプログラムを図１６に示す。

【０１１７】図１７は、本実施形態の信頼性評価装置の構成を示す図である。また、図１８は、本信頼性評価装置による信頼性評価処理の手順を示すフローチャートである。

【０１１８】信頼性評価装置は、受信側の端末装置内に設けられる。図１７に示すように、信頼性評価装置は、文字数計数部２０１、信頼性計算部２０２、評価部２０３を備えている。

【０１１９】まず、文字数計数部２０１により、１つの署名文から１文字づつ取り出され（ステップＳ２０１）、印字可能かどうか判定される（ステップＳ２０２）。印字可能ならばｍに１を加え（ステップＳ２０４）、印字不可能ならばｋに１が加えられる（ステップＳ２０３）。ステップＳ２０１、ステップＳ２０２とステップＳ２０３またはステップＳ２０４の処理を、ステップＳ２０５で１つの署名文が終わるまで繰り返すことにより、印字可能な文字の数ｍと印字不可能な文字の数ｋを数え上げる。

【０１２０】次に、信頼性計算部２０２は、例えば図１６で示したプログラムにより信頼性を計算する（ステップＳ２０６）。そして、評価部２０３では、求められた信頼性の値が一定のしきい値（ここでは０．０００１）以下であるかを判定する（ステップＳ２０７）。信頼性の値がしきい値より大きければ改ざんされた可能性がある旨のメッセージを表示装置（図示せず）に表示するなどして警告を発する（ステップＳ２０８）。

【０１２１】この信頼性評価処理の後に、所定の電子署名検証処理（例えば図２１の従来の電子署名検証あるいは第１の実施形態の電子署名検証など）が行われる（ステップＳ２０９）。

【０１２２】以上のように本実施形態によれば、印字可能文字の総数と印字不可能文字の総数をもとに電子署名の信頼性を計算し、改ざんの可能性を評価することができる。そして、必要に応じて警告を発するなどして注意を促すことができる。

【０１２３】なお、以上の各実施形態における各装置は、ハードウェアで構成することもできるが、各処理を行う部分をソフトウェアで構成することもできる。また、例えば、相当する処理手順を実行させるプログラム

を、コンピュータを制御するためのプログラムとしてコンピュータ読取可能な記憶媒体に格納し、コンピュータに該記憶媒体からプログラムを読取らせ、コンピュータ上で実行させることが可能である。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１２４】

【発明の効果】本発明によれば、署名対象となる電子化文書を複数の署名文に分割し、署名文単位に電子署名を付加するので、電子化文書から署名文・電子署名対の単位で引用することが可能となる。

【０１２５】また、本発明によれば、署名情報を付加する対象となる文書中から予め定められた特定文字を除外して署名情報を生成するので、特定文字を適宜設定することにより、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる。

【０１２６】また、本発明によれば、印字された後も電子署名による改ざん防止に役立つ。また、本発明によれば、印字可能文字の総数と印字不可能文字の総数をもとに電子署名の信頼性を計算し、改ざんの可能性を評価することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る電子署名付加装置の構成を示す図

【図２】同実施形態の署名付加処理の手順を示すフローチャート

【図３】区切り文字検出部による署名文生成処理手順の一例を示すフローチャート

【図４】署名つき文の一例を示す図

【図５】同実施形態の電子署名検証装置の構成を示す図

【図６】同実施形態の署名検証処理の手順を示すフローチャート

【図７】同実施形態の他の署名検証処理の手順を示すフローチャート

【図８】本発明の第２の実施形態に係る電子署名付加装置の構成を示す図

【図９】同実施形態の署名付加処理の手順を示すフローチャート

【図１０】区切り文字検出部による処理後署名文生成処*理手順の一例を示すフローチャート

【図１１】ＡＳＣＩＩコードにおける印字不可能文字を示す図

【図１２】同実施形態の電子署名検証装置の構成を示す図

【図１３】同実施形態の署名検証処理の手順を示すフローチャート

【図１４】同実施形態の他の署名検証処理の手順を示すフローチャート

【図１５】１万分の１以下の確率で改ざんが可能になると考えられる印字不可能な文字の最大数を、文書の文字数（有効文字数）とダイジェストのビット長をパラメータに計算した結果を示す図

【図１６】署名信頼度計算プログラムの一例を示す図

【図１７】本発明の第３の実施形態に係る信頼性評価装置の構成を示す図

【図１８】同実施形態の信頼性評価処理の手順を示すフローチャート

【図１９】従来の電子署名の仕組みを説明するための概念図

【図２０】従来の電子署名付加方法を説明するための流れ図

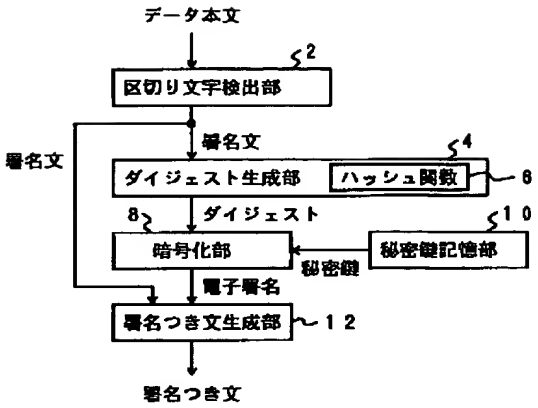
【図２１】従来の電子署名検証方法を説明するための流れ図

【図２２】従来の電子署名における文章の部分引用を説明するための図

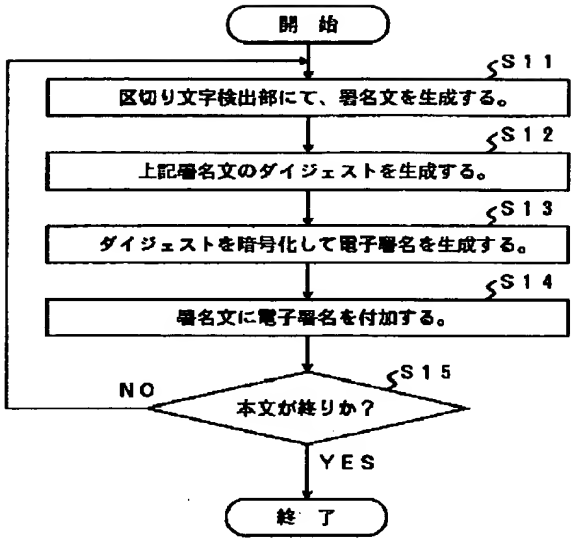
【符号の説明】

２，１０２…区切り文字検出部
４，２４，１０４，１２４…ダイジェスト生成部４
６，２６，１０６，１２６…ハッシュ関数６
８，１０８…暗号化部
１０，１１０…秘密鍵記憶部
１２，１１２…署名つき文生成部
２２，１２２…署名分割部
２８，１２８…復号部
３０，１３０…公開鍵記憶部
１３２，３２…比較部
１０３，１２３…印字不可能文字除外部
２０１…文字数計数部
２０２…信頼性計算部
２０３…評価部

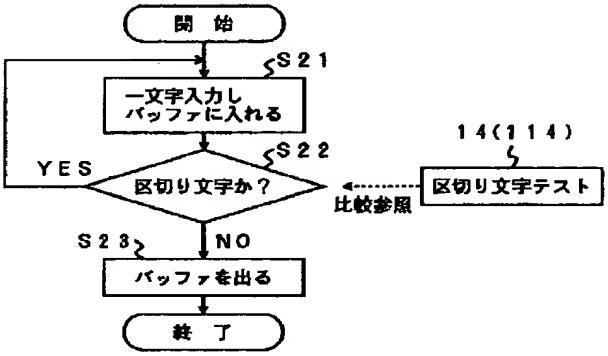
【図１】



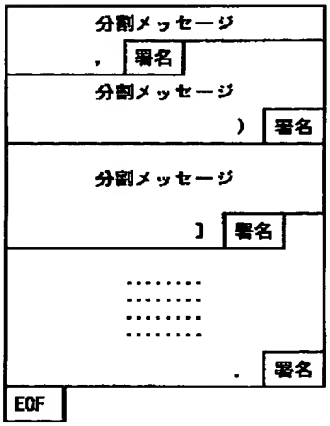
【図２】



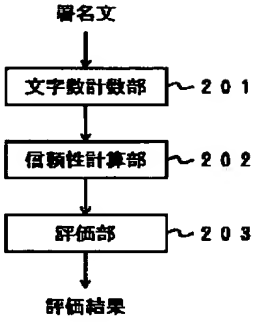
【図３】



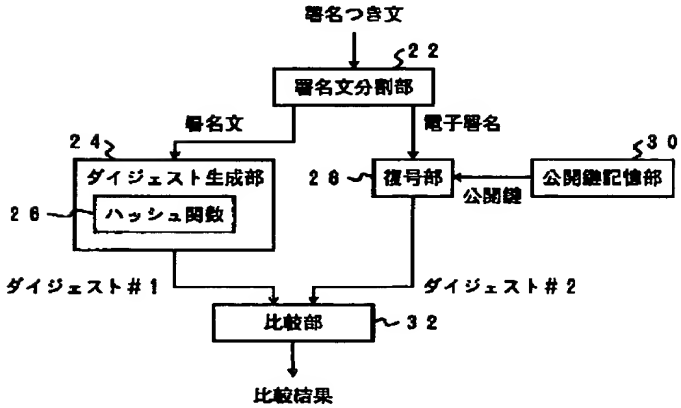
【図４】



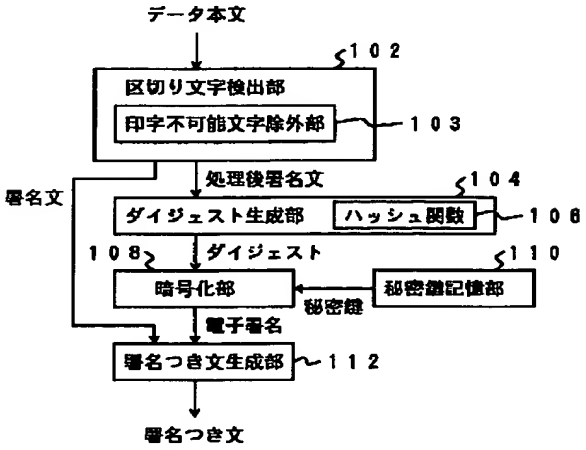
【図１７】



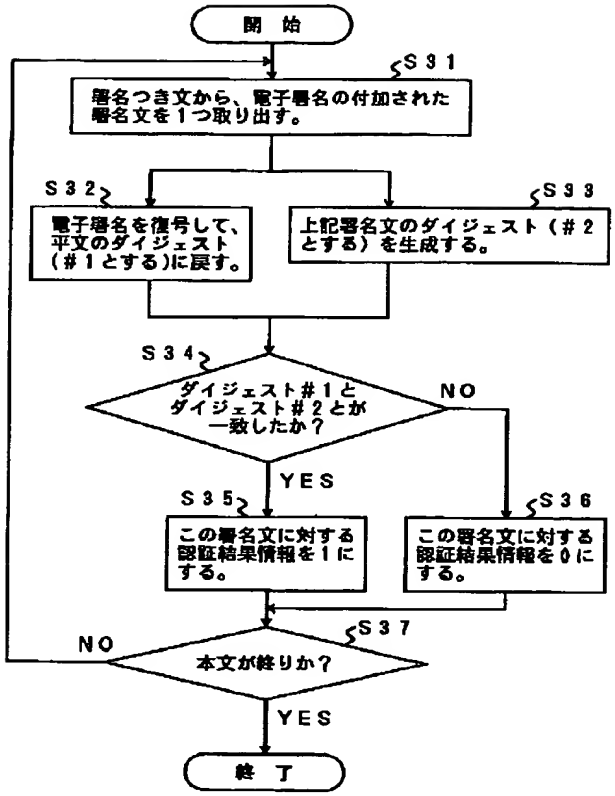
【図５】



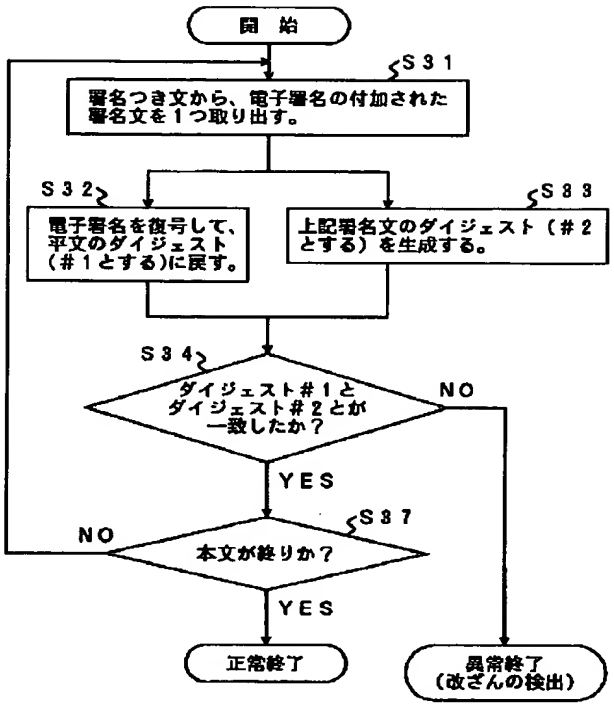
【図８】



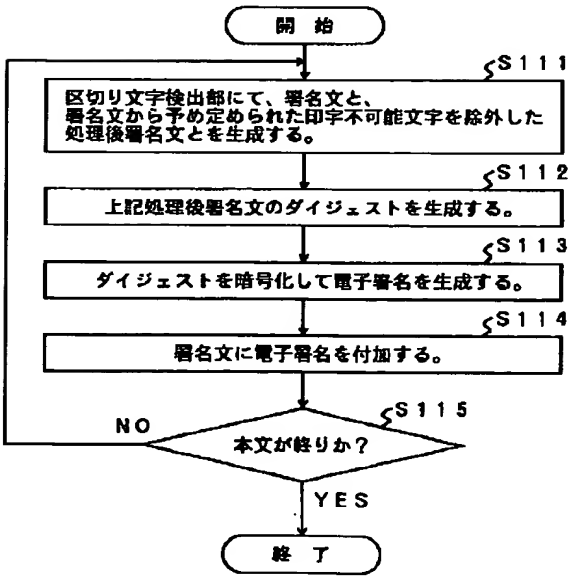
【図６】


開　始
S31
署名つき文から、電子署名の付加された署名文を１つ取り出す。
S32
電子署名を復号して、平文のダイジェスト（＃１とする）に戻す。
S33
上記署名文のダイジェスト（＃２とする）を生成する。
S34
ダイジェスト＃１とダイジェスト＃２とが一致したか？
NO
YES
S35
この署名文に対する認証結果情報を１にする。
S36
この署名文に対する認証結果情報を０にする。
S37
本文が終りか？
NO
YES
終　了

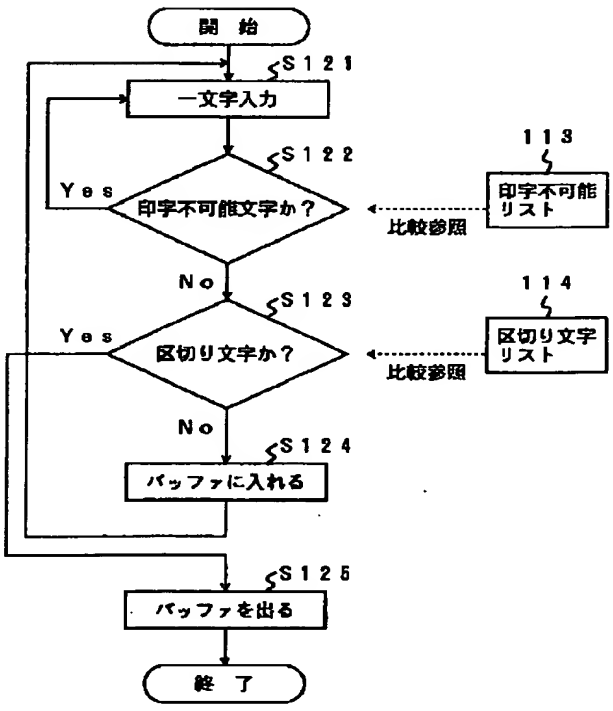
【図７】


開　始
S31
署名つき文から、電子署名の付加された署名文を１つ取り出す。
S32
電子署名を復号して、平文のダイジェスト（＃１とする）に戻す。
S33
上記署名文のダイジェスト（＃２とする）を生成する。
S34
ダイジェスト＃１とダイジェスト＃２とが一致したか？
NO
YES
S37
本文が終りか？
NO
YES
正常終了
異常終了（改ざんの検出）

【図９】


開　始
S111
区切り文字検出部にて、署名文と、署名文から予め定められた印字不可能文字を除外した処理後署名文とを生成する。
S112
上記処理後署名文のダイジェストを生成する。
S113
ダイジェストを暗号化して電子署名を生成する。
S114
署名文に電子署名を付加する。
S115
本文が終りか？
NO
YES
終　了

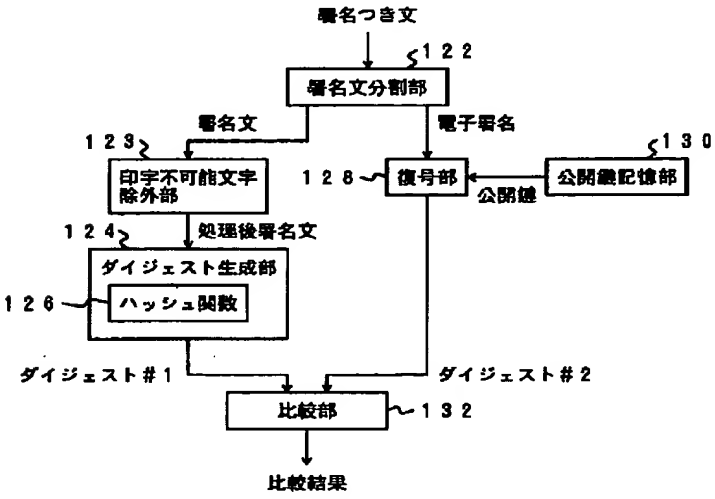
【図１０】


開　始
S121
一文字入力
S122
印字不可能文字か？
Yes
No
113
印字不可能リスト
比較参照
S123
区切り文字か？
Yes
No
114
区切り文字リスト
比較参照
S124
バッファに入れる
S125
バッファを出る
終　了

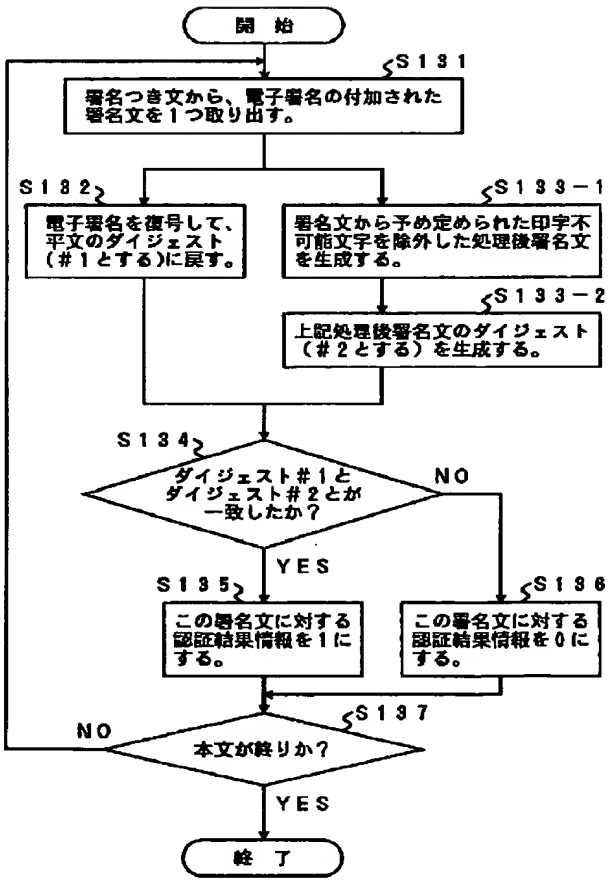
【図１１】

000 nul	001 soh	002 stx	003 etx	004 eot	005 enq	006 ack	007 bel
010 bs	011 ht	012 nl	013 vt	014 np	015 cr	016 so	017 si
020 dle	021 dc1	022 dc2	023 dc3	024 dc4	025 nak	026 syn	027 etb
030 can	031 em	032 sub	033 esc	034 fs	035 gs	036 rs	037 us
040 sp	041 !	042 "	043 #	044 $	045 %	046 &	047 '
050 (	051)	052 *	053 +	054 ,	055 -	056 _	057 /
060 0	061 1	062 2	063 3	064 4	065 5	066 6	067 7
070 8	071 9	072 :	073 ;	074 <	075 =	076 >	077 ?
100 @	101 A	102 B	103 C	104 D	105 E	106 F	107 G
110 H	111 I	112 J	113 K	114 L	115 M	116 N	117 O
120 P	121 Q	122 R	123 S	124 T	125 U	126 V	127 W
130 X	131 Y	132 Z	133 [	134 \	135]	136 ^	137 _
140 '	141 a	142 b	143 c	144 d	145 e	146 f	147 g
150 h	151 i	152 j	153 k	154 l	155 m	156 n	157 o
160 p	161 q	162 r	163 s	164 t	165 u	166 v	167 w
170 x	171 y	172 z	173 {	174 |	175 }	176 ~	177 del

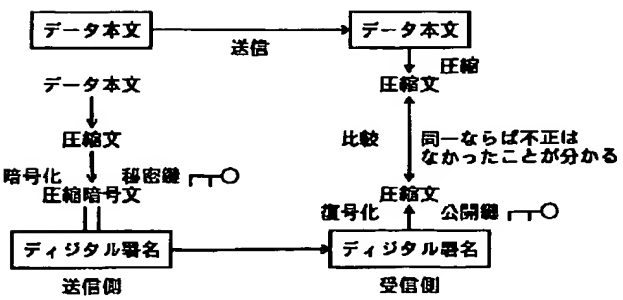
【図１２】



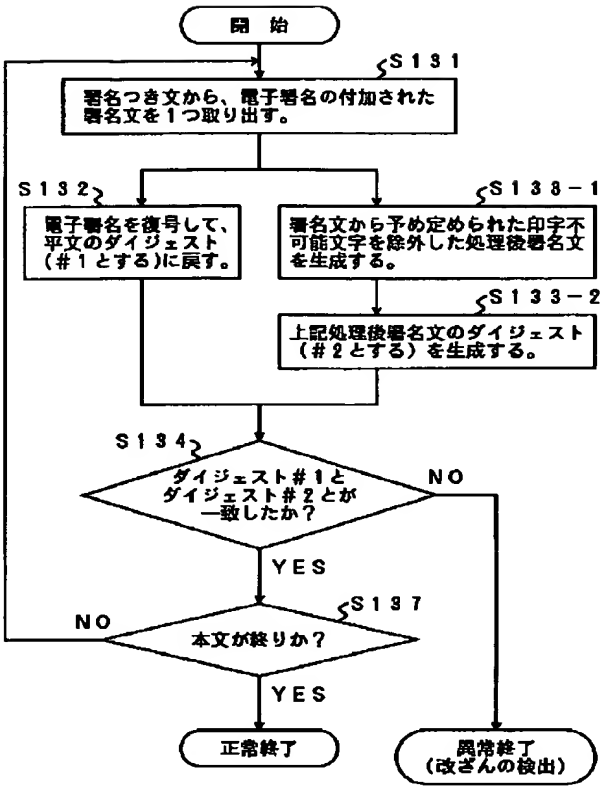
【図１３】



【図１９】



【図１４】



【図１５】

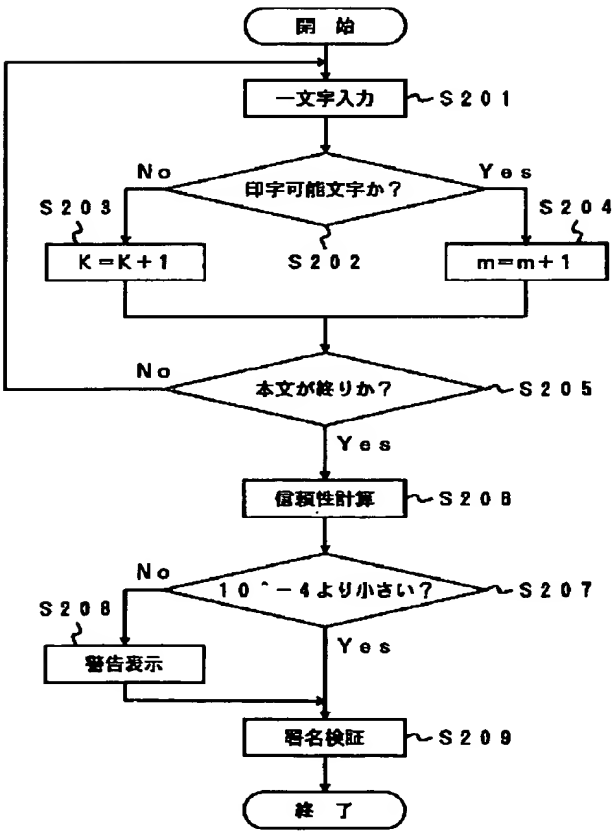
信頼性レベル＝０．０００１００とした最大無効文字数

	ダイジェストのビット長			
有効文字数	３２	６４	１２８	２５６
２＾１	２	６	１４	２７
２＾２	２	６	１３	２６
２＾３	２	５	１２	２５
２＾４	２	５	１１	２４
２＾５	１	４	１１	２３
２＾６	１	４	１０	２１
２＾７	１	４	９	１９
２＾８	１	３	８	１８
２＾９	１	３	８	１７
２＾１０	１	３	７	１６
２＾１１	１	３	７	１５
２＾１２	１	２	６	１４
２＾１３	１	２	６	１３
２＾１４	０	２	６	１２
２＾１５	０	２	５	１２
２＾１６	０	２	５	１１
２＾１７	０	２	５	１０
２＾１８	０	２	４	１０
２＾１９	０	２	４	１０

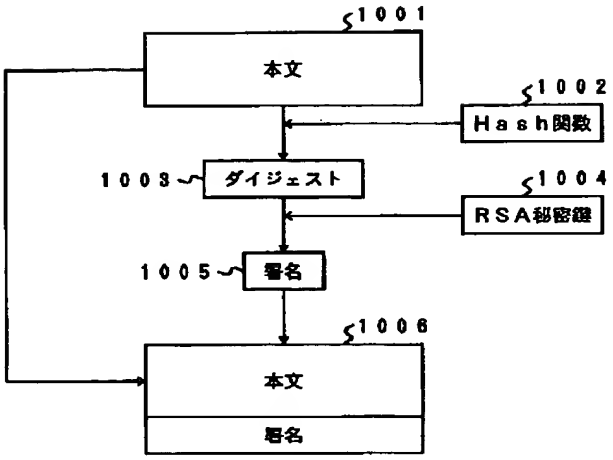
【図１６】

```
#define ILL_CHARS (84)
double lTrustMD(m,k,l)
int m;  /* ダイジェストに有効な文字数    */
int k;  /* ダイジェストに無効な文字数    */
int l;  /* ダイジェストのビット長        */
{
        int i;

        double mdlimit  = pow(2.0,(double)l);
        double var      = 1;

        for ( i=1; i<k+1; i++)
                var = var*ILL_CHARS*(m+i);

        return var/mdlimit;
}
```

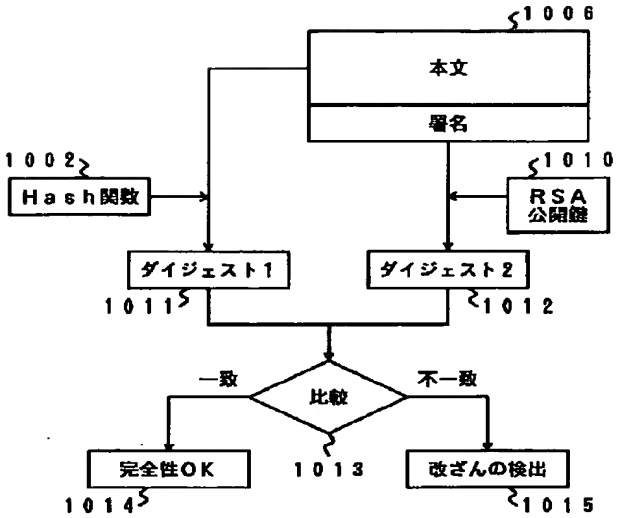
【図１８】



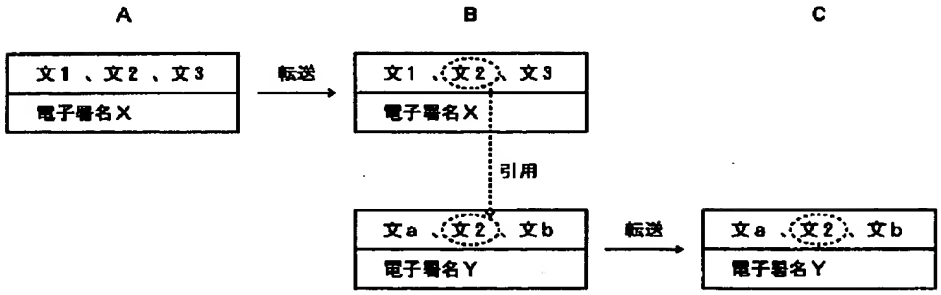
【図２０】


1001
本文
1002
Ｈａｓｈ関数
1003
ダイジェスト
1004
ＲＳＡ秘密鍵
1005
署名
1006
本文
署名

【図２１】


1006
本文
署名
1002
Ｈａｓｈ関数
1010
ＲＳＡ
公開鍵
ダイジェスト１
ダイジェスト２
1011
1012
一致
比較
不一致
完全性ＯＫ
1013
改ざんの検出
1014
1015

【図２２】


A
B
C
文１、文２、文３
電子署名Ｘ
転送
文１、文２、文３
電子署名Ｘ
引用
文ａ、文２、文ｂ
電子署名Ｙ
転送
文ａ、文２、文ｂ
電子署名Ｙ